

#2

Docket No.: 50023-166

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Kaoru MURASE, et al.

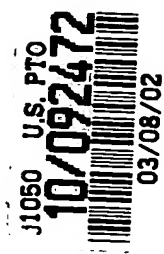
Serial No.:

Group Art Unit:

Filed: March 08, 2002

Examiner:

For: RECORDING AND REPRODUCING DEVICE, CONTROL METHOD AND ABUSE
PREVENTION SYSTEM



**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

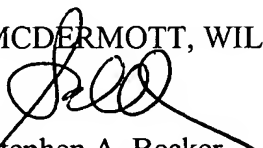
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2001-099850, filed March 30, 2001

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 SAB:mlw
Facsimile: (202)756-8087
Date: March 8, 2002

日本国特許
JAPAN PATENT OFFICE

2002-100
Kaoru MURASE et al.
March 8, 2002
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2001年 3月30日

出願番号
Application Number:

特願2001-099850

出願人
Applicant(s):

松下電器産業株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月26日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3102483

【書類名】 特許願

【整理番号】 2022530091

【提出日】 平成13年 3月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

 【氏名】 村瀬 薫

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

 【氏名】 宮▲ざき▼ 雅也

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100083172

 【弁理士】

 【氏名又は名称】 福井 豊明

【手数料の表示】

 【予納台帳番号】 009483

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9713946

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 記録再生装置、制御方法、及び不正防止システム

【特許請求の範囲】

【請求項 1】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置において、

上記デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知手段と、

上記検知手段による不正利用の検知に基づいて上記記録再生装置の利用を停止する無効化手段と、

を具備することを特徴とする記録再生装置。

【請求項 2】 上記検知手段は、

上記記録されたデジタルコンテンツデータと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、

上記不正防止情報算出手段により算出された不正防止情報を記憶する不正防止情報記憶手段と、

上記不正防止情報記憶手段に記憶された不正防止情報と、上記不正防止情報算出手段が別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段と、

を具備する請求項 1 に記載の記録再生装置。

【請求項 3】 上記検知手段は、

上記記録再生装置を制御する制御プログラムと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、

上記不正防止情報算出手段により算出された不正防止情報を記憶する不正防止情報記憶手段と、

上記不正防止情報記憶手段に記憶された不正防止情報と、上記不正防止情報算出手段が別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段と、

を具備する請求項 1 に記載の記録再生装置。

【請求項 4】 上記検知手段は、不正利用を検知した際に当該検知した旨を所

定の不正検知サーバに送信する請求項 1 ～ 3 のいずれか 1 項に記載の記録再生装置。

【請求項 5】 さらに、記録再生装置を特定する固有 ID を送信する請求項 4 に記載の記録再生装置。

【請求項 6】 上記無効化手段は、上記検知手段より送信される命令により記録再生装置の利用を停止する請求項 1 に記載の記録再生装置。

【請求項 7】 上記無効化手段は、所定の不正検知サーバより送信される命令により記録再生装置の利用を停止する請求項 1 又は 4 に記載の記録再生装置。

【請求項 8】 上記無効化手段は、放送局より送信されるデジタルコンテンツデータに格納される命令により記録再生装置の利用を停止する請求項 1 に記載の記録再生装置。

【請求項 9】 上記無効化手段は、さらに所定の命令により上記利用の停止を解除する請求項 6 ～ 8 のいずれか 1 項に記載の記録再生装置。

【請求項 1 0】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置を制御する制御方法において、

上記デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知ステップと、

上記検知ステップによる不正利用の検知に基づいて上記記録再生装置の利用を停止する無効化ステップと、

を具備することを特徴とする制御方法。

【請求項 1 1】 上記検知ステップは、

上記記録されたデジタルコンテンツデータと所定の関数とを用いて不正防止情報を算出し、不正防止情報記憶手段に記憶する不正防止情報算出ステップと、

上記不正防止情報記憶手段に記憶された不正防止情報と、上記不正防止情報算出ステップが別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較ステップと、

を具備する請求項 1 0 に記載の制御方法。

【請求項 1 2】 上記検知ステップは、

上記記録再生装置を制御する制御プログラムと所定の関数とを用いて不正防止

情報を算出し、不正防止情報記憶手段に記憶する不正防止情報算出ステップと、
 上記不正防止情報記憶手段に記憶された不正防止情報と、上記不正防止情報算出ステップにて別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較ステップと、
 を具備する請求項 1 0 に記載の制御方法。

【請求項 1 3】 上記検知ステップは、不正利用を検知した際に当該検知した旨を所定の不正検知サーバに送信する送信ステップを具備する請求項 1 0 ～ 1 2 のいずれか 1 項に記載の制御方法。

【請求項 1 4】 上記無効化ステップは、所定の不正検知サーバより送信される命令により記録再生装置の利用を停止する請求項 1 0 又は 1 3 に記載の制御方法。

【請求項 1 5】 上記無効化ステップは、放送局より送信されるデジタルコンテンツデータに格納される命令により記録再生装置の利用を停止する請求項 1 0 に記載の制御方法。

【請求項 1 6】 上記無効化ステップは、さらに所定の命令により上記利用の停止を解除する解除ステップを具備する請求項 1 4 又は 1 5 に記載の制御方法。

【請求項 1 7】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置を制御するコンピュータに、

上記デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知ステップと、

上記検知ステップによる不正利用の検知に基づいて上記記録再生装置の利用を停止する無効化ステップと、
 を実行させることを特徴とするプログラム。

【請求項 1 8】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置を制御するコンピュータに、

上記デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知ステップと、

上記検知ステップによる不正利用の検知に基づいて上記記録再生装置の利用を停止する無効化ステップと、

を実行させるプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 1 9】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置に備えられる不正検知装置において、

上記記録されたデジタルコンテンツデータと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、

上記不正防止情報算出手段により算出された不正防止情報を記憶する不正防止情報記憶手段と、

上記不正防止情報記憶手段に記憶された不正防止情報と、上記不正防止情報算出手段が別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段と、

を具備することを特徴とする不正検知装置。

【請求項 2 0】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置に備えられる不正検知装置において、

上記記録再生装置を制御する制御プログラムと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、

上記不正防止情報算出手段により算出された不正防止情報を記憶する不正防止情報記憶手段と、

上記不正防止情報記憶手段に記憶された不正防止情報と上記不正防止情報算出手段が算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段と、

を具備することを特徴とする不正検知装置。

【請求項 2 1】 さらに、不正利用を検知した際に当該検知した旨を所定の不正検知サーバに送信する請求項 1 9 又は 2 0 に記載の不正検知装置。

【請求項 2 2】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置に備えられる無効化装置において、

所定の不正検知サーバより送信される命令に基づいて記録再生装置の利用を停止することを特徴とする無効化装置。

【請求項 2 3】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置に備えられる無効化装置において、

放送局より送信されるデジタルコンテンツデータに格納される命令により再生装置の利用を停止することを特徴とする無効化装置。

【請求項 2 4】 さらに所定の命令により上記利用の停止を解除する請求項 2 2 又は 2 3 に記載の無効化装置。

【請求項 2 5】 所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置における該デジタルコンテンツデータの不正利用を防止する不正利用防止システムにおいて、

上記記録再生装置は、

上記デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知手段と、

所定の時間間隔をもって上記検知手段が検知した不正利用の有又は無を所定の不正検知サーバに送信する送信手段と、

上記不正検知サーバより送信される命令により上記記録再生装置の利用の可否を決定する無効化手段とを備え、

上記不正検知サーバは、

上記記録再生装置より送信された不正利用の有又は無に対応して上記記録再生装置の利用の可否を決定し、当該決定に応じた命令を上記記録再生装置に送信することを特徴とする不正利用防止システム。

【請求項 2 6】 上記記録再生装置は、上記不正検知サーバより送信される、動作を可能とする制御命令を以って所定期間動作可能となる請求項 2 5 に記載の不正利用防止システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、記録再生装置、制御方法、及び不正防止システムに関し、特に、著作権を有するデジタルコンテンツデータの不正利用を防止する記録再生装置、制御方法、及び不正防止システムに関する。

【 0 0 0 2 】

【従来の技術】

近年、情報伝達の手段がデジタル化されつつある。既に放送分野では、そのメリットが多大なことから、アナログ放送からデジタル放送へ移行しつつある。デジタル放送のアナログ放送に対するメリットとしては、多チャンネル化、高画質化等が容易であることが挙げられ、さらに双方向通信のサービスまで視野に入れている。この背景には、特に画像、音声等のデジタルコンテンツデータの規格化による影響が大きく、既にMPEG (Moving Picture Experts Group) によりMPEG1 (CD-ROM等の蓄積メディアのための動画圧縮)、MPEG2 (HDTV (High Definition TeleVision) の制作、送信に対応した動画圧縮)、MPEG4 (低速ネットワークに対応した動画圧縮) 等が制定されている。このような中、例えば放送分野では、上記MPEG2を用いてデータを送信(放送)し、受信側ではアンテナやケーブル等を介してSTB (Set Top Box) と呼ばれるMPEG2のデコード機能を備えた機器にて上記データを受信し再生する。

【0003】

このような場合には、上記送信側ではデジタルコンテンツデータを暗号化して供給し、例えば著作権料を支払う契約等をしている正規ユーザの使用する機器のみに復号のための復号鍵を付与することで正規ユーザのみが上記デジタルコンテンツデータを利用(視聴)可能としている。

【0004】

また更に、上記デジタル放送を、従来のアナログ放送と同様に記録(蓄積)可能であることが求められている。記録に関しては、受信するデータがデジタルコンテンツデータであることより、画像、音声を劣化させることなく容易に行うことが可能である。しかしながら上記記録したデータは劣化することなく複製が可能であることから著作権の問題が生じ、上記記録(蓄積)したデータの扱いに関する著作権問題を解決するための技術が必要不可欠となっている。

【0005】

著作権を有する情報(デジタルコンテンツデータ)に関して上記著作権問題を解決するための代表的な技術に、例えばIEEE1394等を用いたデジタル機器にて採用されているDTC P (Digital Transmission Content Protection)

がある。当該技術は、デジタルコンテンツデータの送受信に関する技術であり、デジタルコンテンツデータにコピー制御情報（CCI）としてコピー禁止（Copy Never、No More Copies）、1世代に限りコピー可能（Copy One Generation）、コピー自由（Copy Free）の情報をもち、上記コピー制御情報に基づいてコピー元機器及びコピー先機器（記憶媒体）で認証処理を行い、問題がなければ暗号化されたデジタルコンテンツデータ及び暗号化に用いる鍵情報のやり取りを行うことでコピーが可能となる。当然上記「コピー禁止」情報を持つデータに関してはコピー不可能である。以上のように、デジタルコンテンツデータにコピー制御情報を備えることで、著作権保護及びユーザの利便性の向上を両立している。

【0006】

また、以下の問題等を考慮し、さらに上記コピー制御情報を拡張しようとする動きがある。即ち、例えば入手した記録媒体に記録されているデジタルコンテンツデータが「1世代に限りコピー可能」である場合には、ユーザは、デジタルコンテンツデータを一旦記録媒体に記録してしまうと、後に異なる記録媒体に移動することが出来ないといった事態が発生する。具体的には、ユーザが受信した「1世代に限りコピー可能」のデジタルコンテンツデータを記録媒体に保存する場合、通常HDD（ハードディスクドライブ）等のアクセス速度が速く使い勝手のよい固定記録媒体に保存する。しかしながら、上記固定記録媒体の記録容量は限られており、またHDD等の固定記録媒体は絶えず使用されている等の理由からリムーバブルな他の記録媒体に比べて破損する可能性が高い。このためユーザが一旦視聴する等して長期に保存したいと判断したデジタルコンテンツデータは、記録容量が限られず保存の面で有利な例えばDVD-RW等のリムーバブルな記録媒体に移動することが望ましい。

【0007】

しかしながら、一旦保存したデジタルコンテンツデータはコピー禁止（No More Copies）になっており、即ちHDDから移動することが出来ず、当該デジタルコンテンツデータに対する処理は再生及び消去のみとなってしまう。

【0008】

このように、上記コピー制御情報のみではユーザの利便性が低いため、例えば

「移動」(Move)といったコピー制御情報を追加し、ユーザの利便性の向上を図ろうとしているのである。上記「移動」は、デジタルコンテンツデータのあるメディアから異なるメディアに移動することであり、コピー元となるメディアに記録されているデジタルコンテンツデータを確実に使用(再生・コピー等)不可能とする。

【 0 0 0 9 】

【発明が解決しようとする課題】

しかしながら、上述したSTBにデジタルコンテンツデータを蓄積するのに使用されるHDD等は、コストダウンを図るために一般のパーソナルコンピュータに使用されているものと同一のものが利用される傾向にある。このため、当該HDDはパーソナルコンピュータに容易に接続することができ、該パーソナルコンピュータにて利用できる豊富なソフトウェアにより上記HDDに蓄積されるデジタルコンテンツデータの(物理的な)コピーが可能となっている。即ち、図8(a)に示すように、HDD801に記録されているデジタルコンテンツデータ802をHDD803に移動した場合、一旦デジタルコンテンツデータ802が復号され、再度暗号化されてHDD803に記録されるが、この際、HDD801に記録されていたデジタルコンテンツデータ802は消去される。しかしながら、図8(b)に示すように、あらかじめHDD801に格納されているデジタルコンテンツデータ802を、異なるHDD804に(物理的に)複製し、図8(c)に示すように、デジタルコンテンツデータ802を移動することが可能となる。この場合にはHDD804に格納されるデジタルコンテンツデータ805を再度HDD801に(物理的に)複製することで、異なるHDDをSTBに接続することなく、デジタルコンテンツデータを再生可能に複製することができる。また、上記方法では、HDD固有のIDを利用して著作権を保護している場合でも、HDD自体は交換しないため結果として著作権を有する情報の不正な利用が可能になってしまうのである。従って、デジタルコンテンツデータ自体に著作権保護技術を施すのみでは限界があり、より一層強固な著作権保護の仕組みが求められている。

【 0 0 1 0 】

さらに、上述したようなユーザの利便性を高めることは、言い換えると悪意を持つ者に不正利用の機会を与えることになる。即ち、上記「1世代に限りコピー可能」や「移動」といった機能を実施するためには、S T B等のハードウェア側にも当然、当該機能を解釈し実施する仕組みが必要になる。しかしながら機能が複雑化するに伴って、当該機能を解釈し実施する仕組みも複雑化し、悪意を有する者の介入する余地、例えばS T B等の機器に不正改造を施す余地が増えるといえる。特に上記不正改造が行われると、著作権を有する情報を容易に複製できるため、当該不正改造はきわめて悪質な不正行為である。

【0011】

従って本発明は、上記従来の事情に基づいて提案されたものであって、著作権を有する情報が不正に利用された際に当該不正を検出し、必要に応じて不正が行われた機器を無効化することにより、一層強固に著作権を保護する記録再生装置、制御方法、及び不正防止システムを提供することを目的とする。

【0012】

【課題を解決するための手段】

本発明は、上記目的を達成するために以下の手段を採用している。すなわち、本発明は、所定のデジタルコンテンツデータの記録及び再生を行う記録再生装置を前提としている。ここで、検知手段は、デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知し、無効化手段は検知手段による不正利用の検知に基づいて記録再生装置の利用を停止する。

【0013】

従って、検知手段を設けて記録手段に対する不正な改変を検知し、さらに検知手段が不正利用を検知した際には無効化手段が当該記録再生装置の動作を停止するため、著作権を有するデジタルコンテンツデータだけではなく、記録再生装置を含めた両面での一層強固な著作権保護の仕組みを提供することができる。

【0014】

上記デジタルコンテンツデータの不正利用を検知する構成とする場合には、上記検知手段は、記録されたデジタルコンテンツデータと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、不正防止情報算出手段により算

出された不正防止情報を記憶する不正防止情報記憶手段と、不正防止情報記憶手段に記憶された不正防止情報と上記不正防止情報算出手段が別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段とを備える。

【 0 0 1 5 】

また、制御プログラムの不正利用を検知する構成とする場合には、上記検知手段は、上記記録再生装置を制御する制御プログラムと所定の関数とを用いて不正防止情報を算出する不正防止情報算出手段と、不正防止情報算出手段により算出された不正防止情報を記憶する不正防止情報記憶手段と、不正防止情報記憶手段に記憶された不正防止情報と上記不正防止情報算出手段が別途算出した不正防止情報とを必要に応じて比較し当該比較の結果をもって不正利用を判定する比較手段とを備える。

【 0 0 1 6 】

以上により、デジタルコンテンツデータだけではなく、制御プログラムの不正利用を防止することが可能である。

【 0 0 1 7 】

尚、上記構成において、上記検知手段は、不正利用を検知した際に当該検知した旨を所定の不正検知サーバに送信する構成とすることが出来る。この際に、例えば記録再生装置を特定する固有 I D を送信してもよい。

【 0 0 1 8 】

以上の構成では、記録再生装置に対して外部の装置と言える不正検知サーバに、不正利用の状態、及び当該記録再生装置を特定する情報を送信することにより、現在までほとんど分からなかった不正利用の実態を知ることが可能となり、さらに記録再生装置を利用する者に対して、不正利用を牽制するといった効果も有する。

【 0 0 1 9 】

尚、無効化手段が、不正検知サーバより送信される命令や、放送局より送信されるデジタルコンテンツデータに格納される命令により記録再生装置の利用を停止し、さらに所定の命令により上記利用の停止を解除する構成では、遠隔地より

記録再生装置の利用を制御できるため、柔軟な運用が可能となる。

【 0 0 2 0 】

さらに、不正利用防止システムでは、記録再生装置は、デジタルコンテンツデータ又は、上記記録再生装置を制御する制御プログラムの不正利用を検知する検知手段と、所定の時間間隔をもって上記検知手段が検知した不正利用の有又は無を所定の不正検知サーバに送信する送信手段と、上記不正検知サーバより送信される命令により上記記録再生装置の利用の可不可を決定する無効化手段とを備える。又、上記不正検知サーバは、記録再生装置より送信された不正利用の有又は無に対応して記録再生装置の利用の可不可を決定し、当該決定に応じた命令を上記記録再生装置に送信する構成とする。

【 0 0 2 1 】

尚、この構成において、さらに記録再生装置は、上記不正検知サーバより送信される、動作を可能とする制御命令を以って所定期間のみ動作可能とすることで、例えば不正利用の発覚を恐れてネットワークとの接続をしていないユーザによる不正利用も防ぐことが可能になる。

【 0 0 2 2 】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

（実施の形態 1）

以下に図 1、図 2、図 3、図 8 を用いて、本発明に係る記録再生装置にてデジタルコンテンツデータを記録・再生する手順の詳細について説明する。ここにデジタルコンテンツデータとは、音声・映像情報の他に、当該音声・映像を制御する制御情報、暗号化や復号化に利用される鍵、コピー制御情報、利用条件等、著作権保護に関連する情報を含むものである。尚、当該記録再生装置 1 0 1 は、例えば上記従来技術にて説明した S T B として提供される。また、該記録再生装置 1 0 1 を構成する各手段は、制御手段 1 0 6 にて管理されており、当該制御手段 1 0 6 は、CPU が不揮発性メモリ（ROM 等）に格納される制御プログラムを

随時読み出して実行することで、各手段の制御を行っている。

【 0 0 2 3 】

最初に、放送局等により放送された番組（デジタルコンテンツデータ）の再生方法について説明する。まず、受信装置 1 0 3 は、放送局により放送（送信）された搬送波を通信衛星及びアンテナ 1 0 2 等を介して受信し、予め決められた規則に従って T S パケット（トランスポートストリームパケット）を生成する。尚、上記 T S パケットは、M P E G 2 にて規格化されているため詳細は省略する。

【 0 0 2 4 】

次に、生成された上記 T S パケットは、上記記録再生装置 1 0 1 を構成するトランスポートストリームデコーダ 1 0 4 に順次送信される。上記 T S パケットを受信したトランスポートストリームデコーダ 1 0 4 は、上記 T S パケットにスクランブルが施されている場合には、必要に応じて所定の復号鍵を用いてデスクランブルしてデジタルコンテンツデータを生成する。尚、上記デスクランブルが施されている際には、例えば上記デジタルコンテンツデータの正当な利用者であるかの認証が記録再生装置の端末 I D 等を用いて行われる。ここに、上記デジタルコンテンツデータとは、放送番組である映像データや音声データ、さらには当該放送番組を構成する映像データや音声データの再生を制御する制御情報、利用者の認証情報、上記コピー制御情報等も含まれる。

【 0 0 2 5 】

続いて上記デジタルコンテンツデータは、A V デコーダ 1 0 5 にて映像出力信号や音声出力信号に変換されて、例えば T V 等のモニタ 1 0 8 に送信され、当該モニタ 1 0 8 は上記各信号を再生する。

【 0 0 2 6 】

また更に、上記デジタルコンテンツデータを記録する際には、トランスポートストリームデコーダ 1 0 4 より出力されたデジタルコンテンツデータを必要に応じて暗復号エンジン 1 0 9 が暗号化し、書込手段 1 1 0 が例えば H D D 1 1 2 や D V D 1 1 3 （D V D - R A M 等）の記録手段に記録する。尚、この際に、コピー制御情報も暗号鍵を用いて暗号化される。上記暗復号エンジン 1 0 9 が上記デジタルコンテンツデータやコピー制御情報を暗号化する際に使用したコンテンツ

鍵は、記録再生装置 1 0 1 固有のセット固有鍵で暗号化され、暗号化コンテンツ鍵として同様に記録手段に記録される。但し、この際に、上記デジタルコンテンツデータにおけるコピー制御情報の内容が確認され、例えば「コピー禁止」である場合には、当該デジタルコンテンツデータを記録できないようになっている。

【 0 0 2 7 】

一方、記録手段に記録されたデジタルコンテンツデータを再生する際には、まず読出手段 1 1 1 が、記録手段より目的とするデジタルコンテンツデータを読み出して暗復号エンジン 1 0 9 に送信する。該デジタルコンテンツデータを受信した暗復号エンジン 1 0 9 は、当該デジタルコンテンツデータを復号化して A V デコーダ 1 0 5 に送信し、A V デコーダ 1 0 5 は、デジタルコンテンツデータを映像出力信号や音声出力信号に変換して、例えば T V 等のモニタ 1 0 8 に送信する。続いて当該モニタ 1 0 8 は上記各信号を再生する。

【 0 0 2 8 】

以上の処理により、デジタルコンテンツデータの再生・記録が行われる。また、デジタル放送では双方向通信を利用した様々な放送形態が企画されており、送受信手段 1 1 4 を備えることで、例えばインターネット等のネットワーク 1 1 5 と通信可能に接続されている。尚、上記各手段は、従来における一般的な記録再生装置を構成する手段と同様である。

【 0 0 2 9 】

ここで本実施の形態 1 に係る記録再生装置 1 0 1 は、さらに検知手段 1 1 6、及び無効化手段 1 1 7 を備える。尚、図 2 は、本実施の形態 1 における検知手段 1 1 6 の概略機能ブロック図である。

【 0 0 3 0 】

続いて、以下にデジタルコンテンツデータが例えば H D D 1 1 2 に記録されている状態における検知手段 1 1 6、及び無効化手段 1 1 7 の処理の詳細について説明する。

【 0 0 3 1 】

上記記録再生装置 1 0 1 が通常運用されている場合には、まず、検知手段 1 1 6 は、記録再生装置 1 0 1 の電源オフがされたかどうかを判断する（図 3（a）

: S 3 0 1)。

【0032】

ここで、電源オフされた場合、読出手段111を介して所定のタイミングで例えばHDD112に記録されているデジタルコンテンツデータを読出す(図3(a): S301 Yes → S302)。尚、上記読出すデジタルコンテンツデータは、記録されているデジタルコンテンツデータすべてであってもよいし、暗号化や復号化に利用される鍵、コピー制御情報、利用条件等、著作権保護に関連する情報のみでもよい。上記利用条件とは、例えばデジタルコンテンツデータの再生可能回数や、再生期限を示した情報である。

【0033】

上記デジタルコンテンツデータを受信した検知手段116を構成する不正防止情報算出手段201は、例えばハッシュ関数を用いて上記デジタルコンテンツデータのハッシュ値(不正防止情報)を算出する(図3(a): S303)。ここで、上記ハッシュ関数を用いると、上記受信したデジタルコンテンツデータから算出される不正防止情報は、当該デジタルコンテンツデータが変更(改変)されない限り同一の値となる情報であり、且つ当該不正防止情報から上記デジタルコンテンツデータを算出することは不可能な情報である。尚、デジタルコンテンツデータのサイズが大きな場合等には、上述したように当該デジタルコンテンツデータの著作権保護に比較的重要な部分、即ち暗号化コンテンツ鍵、コピー制御情報、コンテンツID(記録時のファイル名)等の必要最小限のみのハッシュ値を算出してもよい。

【0034】

上記デジタルコンテンツデータに対する不正防止情報を算出した不正防止情報算出手段201は、当該不正防止情報を、検知手段116を構成する不正防止情報記憶手段202に格納する(図3(a): S304)。尚、不正防止情報記憶手段202は、具体的には不揮発性記憶装置(例えばRAM)等であり、記録手段とは別媒体として構成される。

【0035】

上記処理により、HDD112内に記録されているデジタルコンテンツデータ

の不正防止情報は随時不正防止情報記憶手段 2 0 2 に格納されることになる。尚、上記処理 S 3 0 1 ~ S 3 0 4 は上記記録再生装置 1 0 1 の電源オフ時に実行されるものであるが、その他、例えば所定のタイミング毎に繰り返してもよい。該所定のタイミングとは、例えば上記 HDD 1 1 2 内のデジタルコンテンツデータが更新された時や、一定の時間間隔毎である。

【 0 0 3 6 】

上記更新された時の処理を、図 8 を用いて簡単に説明する。図 8 (a) において、HDD 8 0 1 からデジタルコンテンツデータ 8 0 2 を HDD 8 0 3 に移動した場合を考える。当初、STB 内の不正防止情報記憶手段 2 0 2 には、移動前における HDD 8 0 1 の不正防止情報が記録されている。ここで、HDD 8 0 1 からデジタルコンテンツデータ 8 0 2 が HDD 8 0 3 に移動されると、移動後は HDD 8 0 1 内のデジタルコンテンツデータ 8 0 2 は消去される。即ち、上記 HDD 8 0 1 は更新されたことになる。該 HDD 8 0 1 が更新されると、当該更新された旨が例えば制御手段 1 0 6 から検知手段 1 1 6 に送信され、上記更新された旨の情報を受信した検知手段 1 1 6 は、HDD 8 0 1 内のデジタルコンテンツデータを読み出し、不正防止情報算出手段 2 0 1 が再度不正防止情報を計算し不正防止情報記憶手段 2 0 2 に格納する。以上により、HDD 内に記録されているデジタルコンテンツデータの不正防止情報は随時不正防止情報記憶手段 2 0 2 に格納されることになる。

【 0 0 3 7 】

さて、上記記録再生装置 1 0 1 の通常運用時の動作は上記に示したが、例えば上記記録再生手段 1 0 1 の電源が一旦オフにされた後、再度電源がオンにされた際には、図 3 (b) に示す電源オン処理が実行される。

【 0 0 3 8 】

即ち、電源オン時の処理ではある場合、検知手段 1 1 6 は、読出手段 1 1 1 を介して HDD 1 1 2 に記録されているデジタルコンテンツデータを読み出し、当該デジタルコンテンツデータに対応する不正防止情報を算出した後、該不正防止情報を比較手段 2 0 3 に送信する（図 3 (b) : S 3 0 5 → S 3 0 6）。また、一方で、上記比較手段 2 0 3 は、不正防止情報記憶手段 2 0 2 より、すでに記憶さ

れている不正防止情報を読み出す（図 3（b）：S 3 0 7）。

【0 0 3 9】

続いて上記比較手段 2 0 3 は、上記不正防止情報記憶手段 2 0 2 から読み出した不正防止情報と、上記不正防止情報算出手段 2 0 1 が算出した不正防止情報を比較する（図 3（b）：S 3 0 8）。

【0 0 4 0】

ここで、上記 2 つの不正防止情報が同一の場合、HDD 1 1 2 に格納されているデジタルコンテンツデータが、記録再生装置 1 0 1 の電源オフの間に改変されていないことを示し、以後通常の処理 S 3 0 2 ～S 3 0 4 を繰り返す（図 3（b）：S 3 0 9 Yes → 図 3（a）S 3 0 1）。

【0 0 4 1】

ここで、上記 2 つの不正防止情報が異なる場合、HDD 1 1 2 に格納されているデジタルコンテンツデータが、記録再生装置 1 0 1 の電源オフの間に、当該記録再生装置 1 0 1 を介することなく改変されていることを示し、上記比較手段 2 0 3 は当該改変されている旨を無効化手段 1 1 7 に通知する（図 3（b）：S 3 0 9 No → S 3 1 0）。

【0 0 4 2】

上記比較手段 2 0 3 は、具体的には、以下のような不正利用が行われた場合に無効化手段 1 1 7 に通知することになる。即ち、図 8（b）にて、HDD 8 0 1 内のデジタルコンテンツデータ 8 0 2 を HDD 8 0 3 に移動した場合、図 8（c）に示したように、HDD 8 0 1 内のデジタルコンテンツデータは消去されると共に、検知手段 1 1 6 の不正防止情報記憶手段 2 0 2 内の不正防止情報も更新されているはずである。ここで、上記従来技術に説明したように、例えば HDD が物理的に複製された場合には、デジタルコンテンツデータ 8 0 5 を再度 HDD 8 0 1 に複製することにより、HDD 8 0 1 を元の状態（デジタルコンテンツデータ 8 0 2 を有する状態）に戻すことが可能である。しかしながら、これは不正利用であり許されることではない。そこで、不正防止情報記憶手段 2 0 2 に格納されている不正防止情報と、上記元の状態に戻された際の不正防止情報の差異を検知して、不正利用（デジタルコンテンツデータの改変）を検知し無効化手段 1 1

7に通知する。

【0043】

以上により、検知手段116は、記録手段118（例えばHDD112、DVD113等）に対する不正利用、即ちデジタルコンテンツデータの改変を検知することが可能である。

【0044】

尚、上記記録手段118が着脱可能であることが考えられる。このような場合には、上記検知手段116は、当該記録手段に記録されている固有のIDと、上記不正防止情報とを関連付けて不正防止情報記憶手段202に格納することで、記録手段毎に不正利用を検知することが可能となる。

【0045】

又、上記HDDが活抜挿（電源オンの状態での交換）可能である場合には、上記比較手段203は、当該活抜挿が行われた際に不正防止情報を比較する処理（電源オン処理）を行えばよい。

【0046】

続いて、上記検知手段116より、HDD112に格納されているデジタルコンテンツデータが改変されている旨、即ち不正利用が行われている旨の通知を受けた無効化手段117は、記録再生装置101の記録・再生処理を停止する命令を例えば制御手段106に送信し、記録再生装置の利用（動作）を停止する。尚、当該記録再生装置の利用を停止する方法は限定するものではないが、例えば以下のような場合が考えられる。

【0047】

即ち、制御手段106が記録再生装置101を制御する際に、動作フラグをチェックする機能を備え、当該動作フラグが0の場合には通常利用可能とする。この場合には、上記無効化手段117は、上記所定の動作フラグを1とすることで上記記録再生装置101の動作を停止することが可能となる。

【0048】

また、上記制御手段106を機能させる制御プログラムが格納されているROM107の必要部分を消去・改変するといったことも可能である。

【 0 0 4 9 】

また更に、不正防止情報記憶手段 2 0 2 に格納されている不正防止情報の値を変更するといった手法でも、上記記録再生装置 1 0 1 の動作を停止することが可能である。

【 0 0 5 0 】

以上のように、本発明に係る記録再生装置は検知手段を設けて記録手段に対する不正な改変を検知し、さらに検知手段が不正利用を検知した際には無効化手段が当該記録再生装置の動作を停止するため、著作権を有するデジタルコンテンツデータだけではなく、記録再生装置を含めた両面での一層強固な著作権保護の仕組みを提供することができる。

【 0 0 5 1 】

尚、本実施の形態 1 では、一例としてハッシュ関数を用いた例を説明したが、ハッシュ関数に限定する必要は無く、デジタルコンテンツデータから一意の不正防止情報が導き出せる関数であればよい。

(実施の形態 2)

次に、図 4、図 5、図 6、図 7 を用いて、実施の形態 2 における記録再生装置について説明する。尚、実施の形態 2 では、上記実施の形態 1 と共通する点が多いため、異なる点のみを説明する。

【 0 0 5 2 】

まず、本実施の形態 2 では、検知手段 5 0 1 を構成する不正防止情報算出手段 6 0 1 は、ROM 1 0 7 に格納されている制御プログラムを読み出し、不正防止情報を算出して比較手段 6 0 3 に送信する（図 4 (a) : S 4 0 1）。

【 0 0 5 3 】

続いて、比較手段 6 0 3 は、不正防止情報記憶手段 6 0 2 に予め記憶されている上記制御プログラムの不正防止情報を読み出して、該 2 つの不正防止情報を比較する（図 4 (a) : S 4 0 2 → S 4 0 3）。

【 0 0 5 4 】

ここで、上記 2 つの不正防止情報が同一である場合、上記制御プログラムの改変は行われていないため、即ち記録再生装置の不正利用は行われていないと判断

する（図 4（a）：S 4 0 4 Y e s → E n d）。

【0 0 5 5】

ここで、上記 2 つの不正防止情報が異なる場合、上記制御プログラムは改変されているため、即ち記録再生装置に何らかの改造が施され、不正利用が行われていると判断する（図 4（a）：S 4 0 4 N o）。

【0 0 5 6】

この場合、上記実施の形態 1 と同様、無効化手段 5 0 2 に不正利用が行われている旨を送信してもよいが、ここでは送受信手段 5 0 3 を介して不正検知サーバ 7 0 1 に当該不正利用が行われている旨を送信するものとする（図 4（a）：S 4 0 5）。尚、この際に、上記記録再生装置 5 0 0 を識別する固有 I D も同時に送信する。ここで、当該固有 I D とは、上記記録再生装置 5 0 0 を特定可能な情報であり、例えば I P アドレス（インターネットプロトコルアドレス）や製造番号、製品番号等である。

【0 0 5 7】

以上により、検知手段 5 0 1 が検知した、不正利用が行われている旨は、記録再生装置 5 0 0 外である不正検知サーバ 7 0 1 に送信される。

【0 0 5 8】

続いて、上記不正検知サーバ 7 0 1 は、必要に応じて記録再生装置 5 0 0 を構成する無効化手段 5 0 2 に対して、記録再生装置の利用を停止する旨を示す命令を送信し、無効化手段 5 0 2 は上記命令を受けて記録再生装置 5 0 0 の利用を停止する。

【0 0 5 9】

尚、利用を停止する方法は、上述したように上記実施の形態 1 に記載したものと同様でよいが、無効化された記録再生装置を不正検知サーバ（外部）から再度有効化を可能にすることで外部から記録再生装置の利用の制御を可能にし、柔軟な運用形態を実施できるようにしてもよい。この際には、例えば上記実施の形態 1 にて説明した動作フラグを不正検知サーバからの命令により例えば“0”に変更可能にしたり、再度新しい制御プログラムを送信したりすることで実施可能である。

【 0 0 6 0 】

以上のように、本実施の形態 2 における記録再生装置では、検知手段が制御プログラムの改変、即ち不正利用を検知することにより、記録再生装置に対する改造を防ぐことが可能になる。記録再生装置に対する改造は、例えばコピー制御情報による著作権保護の機能を停止する（機能不能にする）といった悪質なものが考えられると共に、著作権を有するデジタルコンテンツデータを大量、且つ容易に不正コピーすることを可能にするため、制御プログラムの改変の防止は著作権保護に非常に有効であるといえる。

【 0 0 6 1 】

また、記録再生装置に対して外部の装置と言える不正検知サーバに、不正利用の状態、及び当該記録再生装置を特定する情報を送信することにより、現在までほとんど分からなかった不正利用の実態を知ることが可能となり、さらに記録再生装置を利用する者に対して、不正利用を牽制するといった効果も有する。

【 0 0 6 2 】

また更に、不正検知サーバ（外部）からの命令により記録再生装置の利用の停止を可能とすることで、例えば不正利用されたデジタルコンテンツデータ（不正コピーされたデジタルコンテンツデータ）の例えば電子透かし等に基づいて、不正利用に関わった記録再生装置を特定できた場合には利用を停止することが可能となる。具体的には、例えば以下のような処理が上げられる。即ち、上記無効化手段 5 0 2 は不正検知サーバより無効化命令を受信すると、不正防止情報記憶手段 6 0 2 に格納されるハッシュ値（不正防止情報）の値を全く異なる値に改変する（図 4（b）：S 4 0 6 → S 4 0 7）。ここで、不正防止情報記憶手段 6 0 2 に格納されるハッシュ値（不正防止情報）を変更することで、以後、検知手段 5 0 1 が格納された不正防止情報と、算出した不正防止情報を比較した場合に不正防止情報が一致しないため、上記制御手段 1 0 6 は記録再生装置 5 0 0 の動作を停止する。

【 0 0 6 3 】

また更に、無効化手段 5 0 2 は、上記不正検知サーバより無効化命令を受信すると、上記実施の形態 1 で示した動作フラグを“1”に変更するのみでも、上記

制御手段 1 0 6 は記録再生装置 5 0 0 の動作を停止する。この場合には、検知手段がなくても記録再生装置 5 0 0 の動作を停止することが可能である。

【 0 0 6 4 】

尚、上記無効化手段 5 0 2 に対して、不正検知サーバから利用を停止する旨を示す命令を送信しているが、例えば不正検知サーバ 7 0 1 に送信された情報を元に、放送局 7 0 2 からアンテナ 1 0 2 及び受信装置 1 0 3 を介して無効化手段に上記停止する旨を示す命令を送信してもよい。

【 0 0 6 5 】

また更に、本実施の形態 2 においては、不正防止情報記憶手段 6 0 2 に予め制御プログラムの不正防止情報を記憶しておくものとしたが、外部から新しい制御プログラムをダウンロードして実行可能とする記録再生装置においては、実施の形態 1 と同様、任意のタイミングで制御プログラムの不正防止情報を計算して不正防止情報記憶手段 6 0 2 に保存するといった方法を用いてもよい。ここで任意のタイミングとは例えば電源オン時であり、該電源オン時に不正防止情報の比較を行い、電源オフ時に不正防止情報記憶手段 6 0 2 への保存を行うといったものでよい。

(実施の形態 3)

次に、図 5、図 7 を用いて、実施の形態 3 における記録再生装置について説明する。尚、実施の形態 2 では、上記実施の形態 1、2 と共通する点が多いため、異なる点のみを説明する。

【 0 0 6 6 】

まず、本実施の形態 3 では、上記検知手段 5 0 1 は、所定のタイミング、例えば一ヶ月に 1 度不正検知サーバに接続し、不正利用の判断結果を送信する。尚、不正利用の判断は、上記実施の形態 1 及び 2 にて行われたものと同様である。

【 0 0 6 7 】

ここで、不正利用がない場合には、次の一ヶ月間の動作を可能とする制御命令を送信するが、不正利用があった場合には、上記動作を可能とする制御命令を送信しない。

【 0 0 6 8 】

以上の運用形態では、例えば不正利用の発覚を恐れてネットワーク 1 1 5 との接続をしていないユーザによる不正利用も防ぐことが可能になる。

【 0 0 6 9 】

尚、不正利用があった場合、直ちにもしくは後日、不正検知サーバ 7 0 1 もしくは放送局 7 0 2 より無効化手段 5 0 2 に対して記録再生装置 5 0 0 の停止命令を送信することで、記録再生装置 5 0 0 を利用不可能としてもよいのは言うまでも無い。

【図面の簡単な説明】

【図 1】

実施の形態 1 における記録再生装置の概略機能ブロック図。

【図 2】

実施の形態 1 における検知手段の概略機能ブロック図。

【図 3】

検知手段の処理を示すフローチャート。

【図 4】

実施の形態 2 における検知及び無効化手段のフローチャート。

【図 5】

実施の形態 2 における記録再生装置の概略機能ブロック図

【図 6】

実施の形態 2 における検知手段の概略機能ブロック図。

【図 7】

不正防止システムの概略構成図。

【図 8】

不正利用を説明するためのイメージ図。

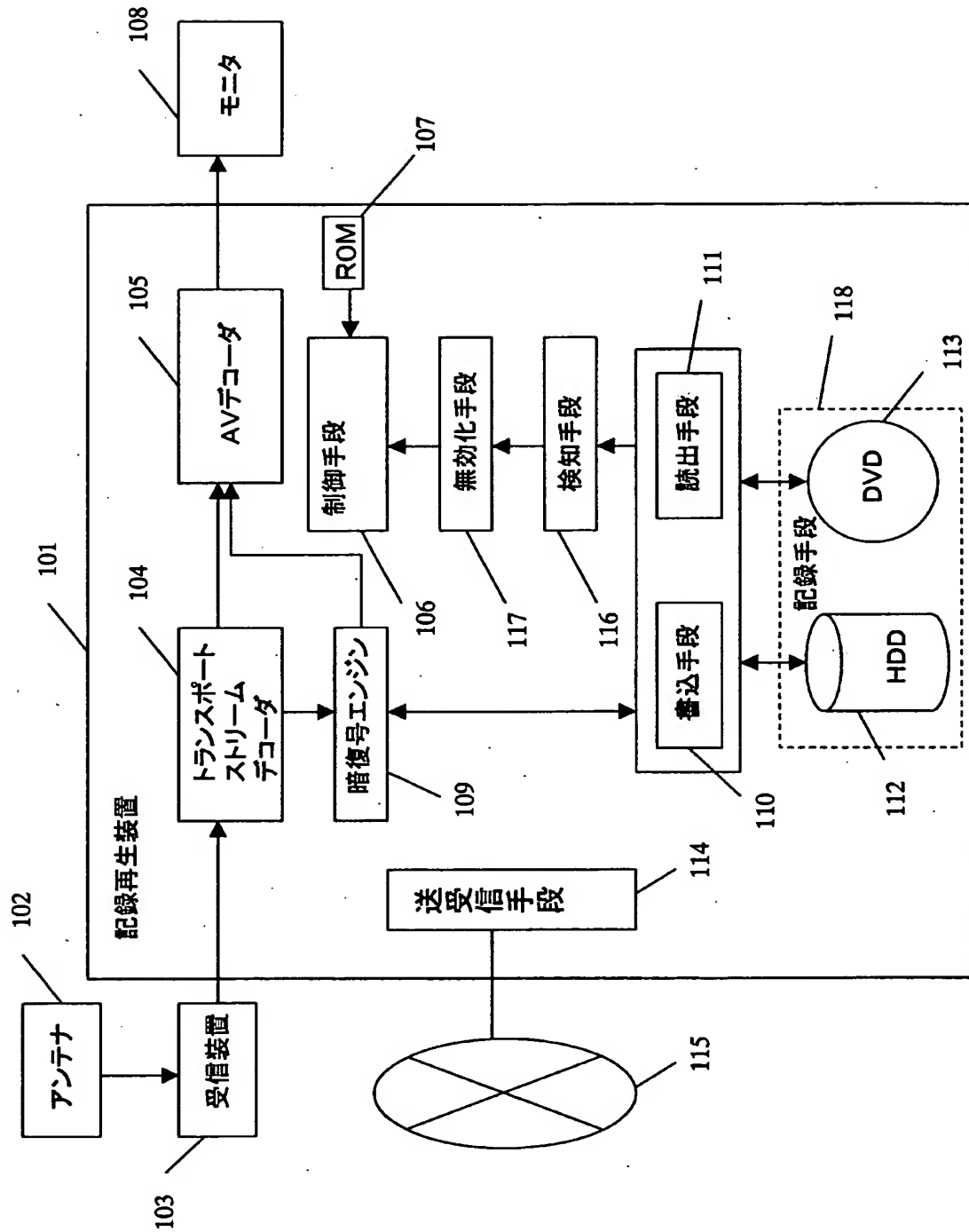
【符号の説明】

- 1 0 1 記録再生装置
- 1 0 2 アンテナ
- 1 0 3 受信装置
- 1 0 4 トランスポートストリームデコーダ

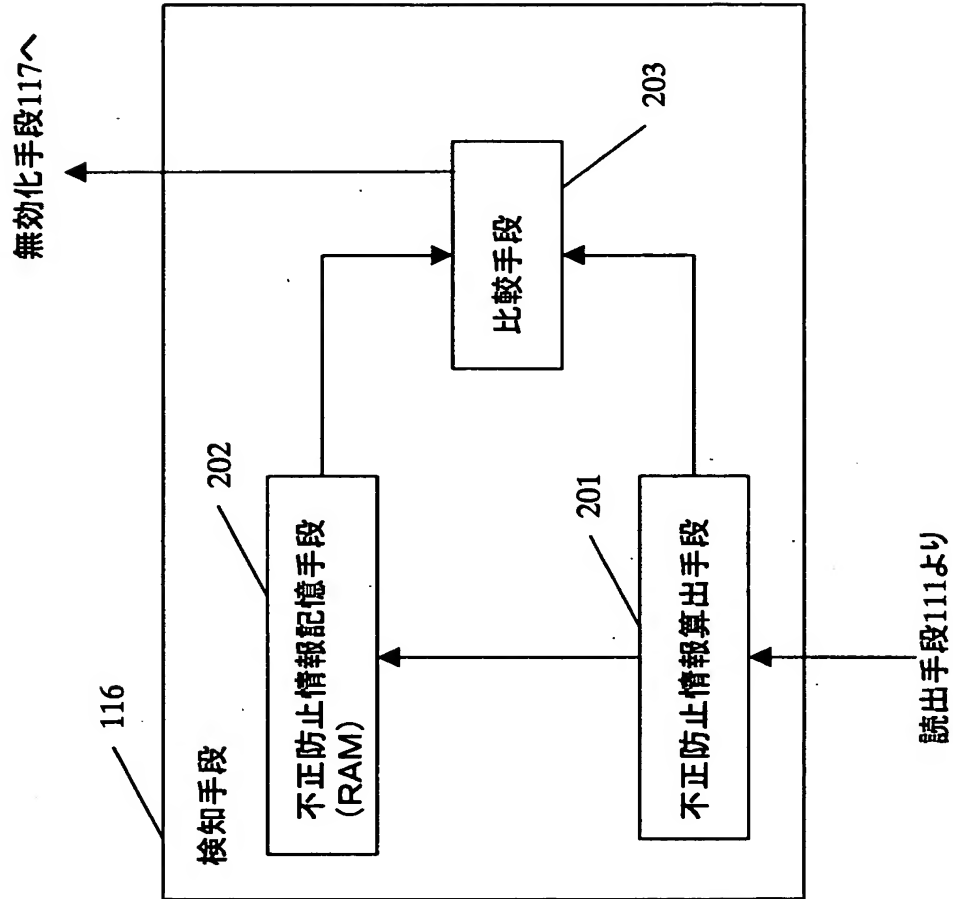
- 1 0 5 A V デ コ ー ダ
- 1 0 6 制 御 手 段
- 1 0 7 R O M
- 1 0 8 モ ニ タ
- 1 0 9 暗 復 号 エ ン ジ ン
- 1 1 0 書 込 手 段
- 1 1 1 読 出 手 段
- 1 1 2 H D D (記 録 手 段 1 1 8 を 構 成)
- 1 1 3 D V D (記 録 手 段 1 1 8 を 構 成)
- 1 1 4 送 受 信 手 段
- 1 1 5 ネ ッ ト ワ ー ク
- 1 1 6 検 知 手 段
- 1 1 7 無 効 化 手 段
- 1 1 8 記 録 手 段

【書類名】 図面

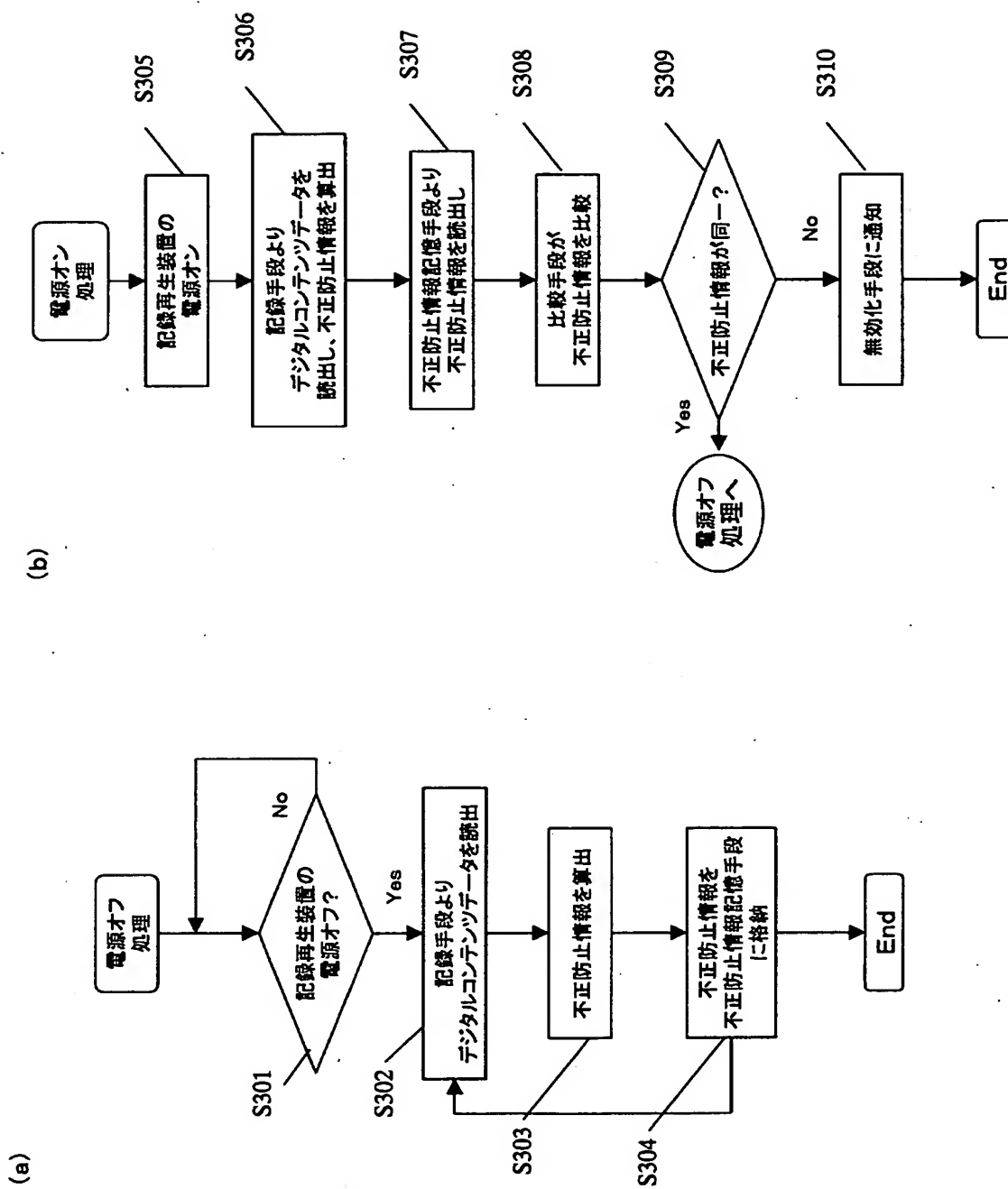
【図 1】



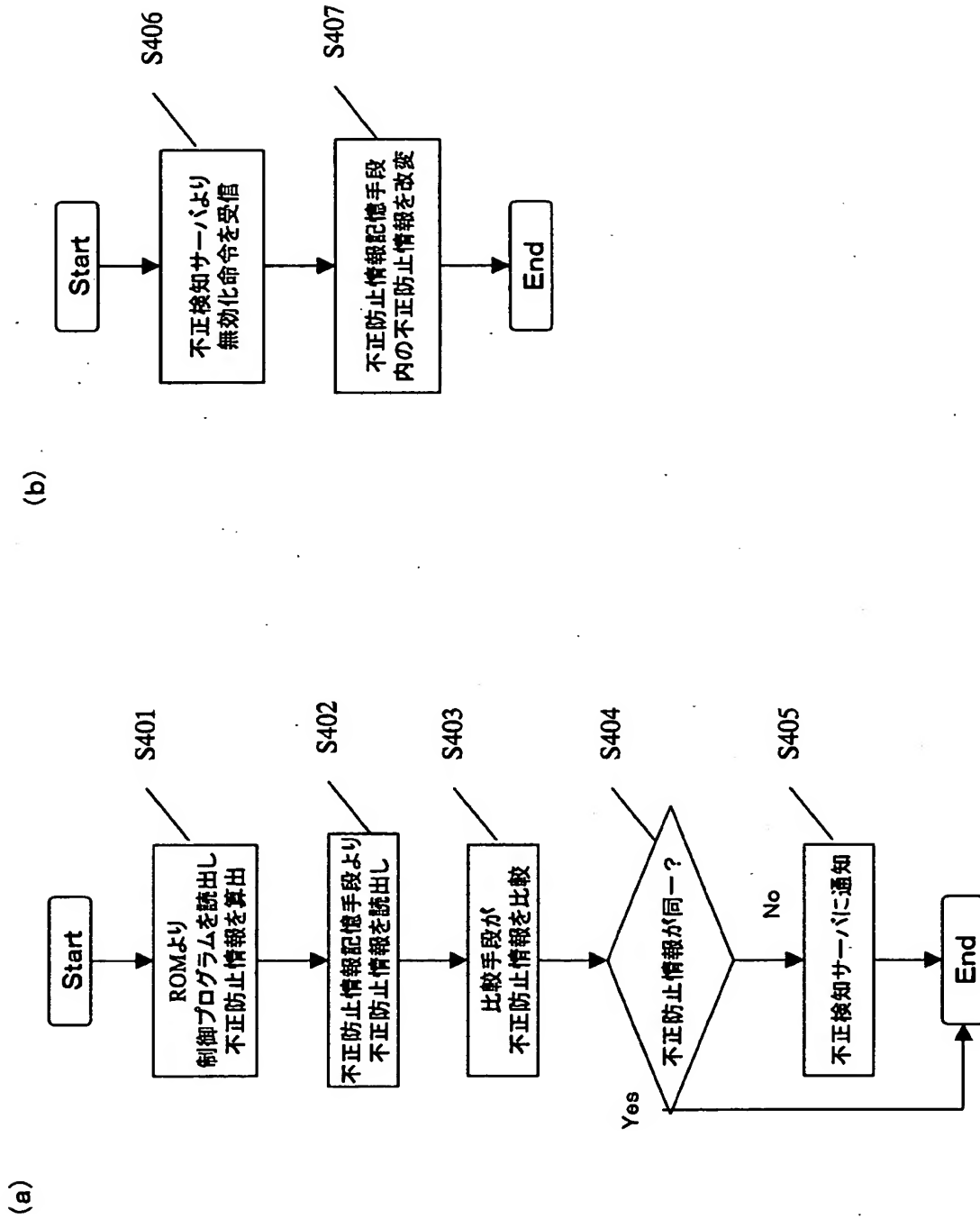
【図 2】



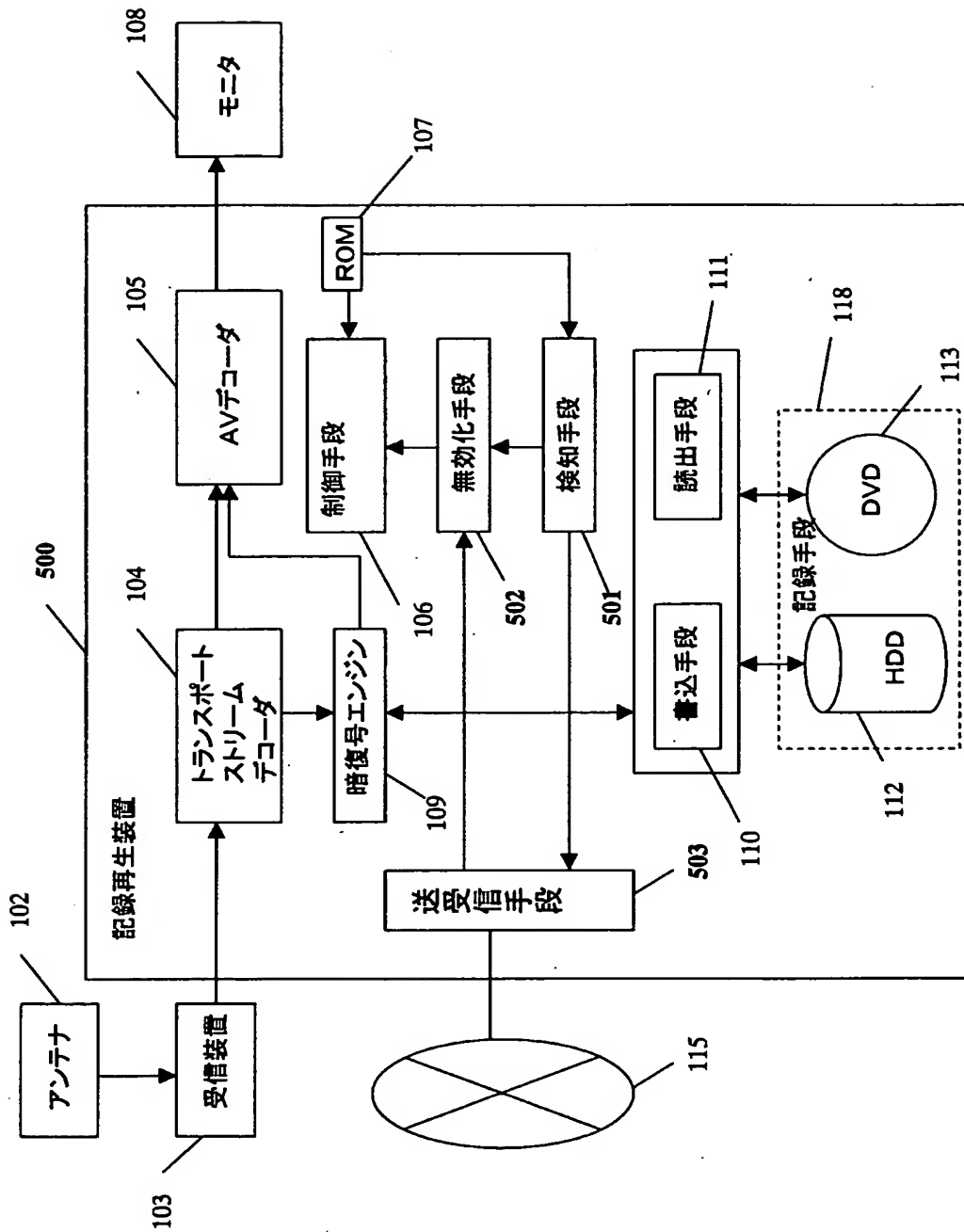
【図 3】



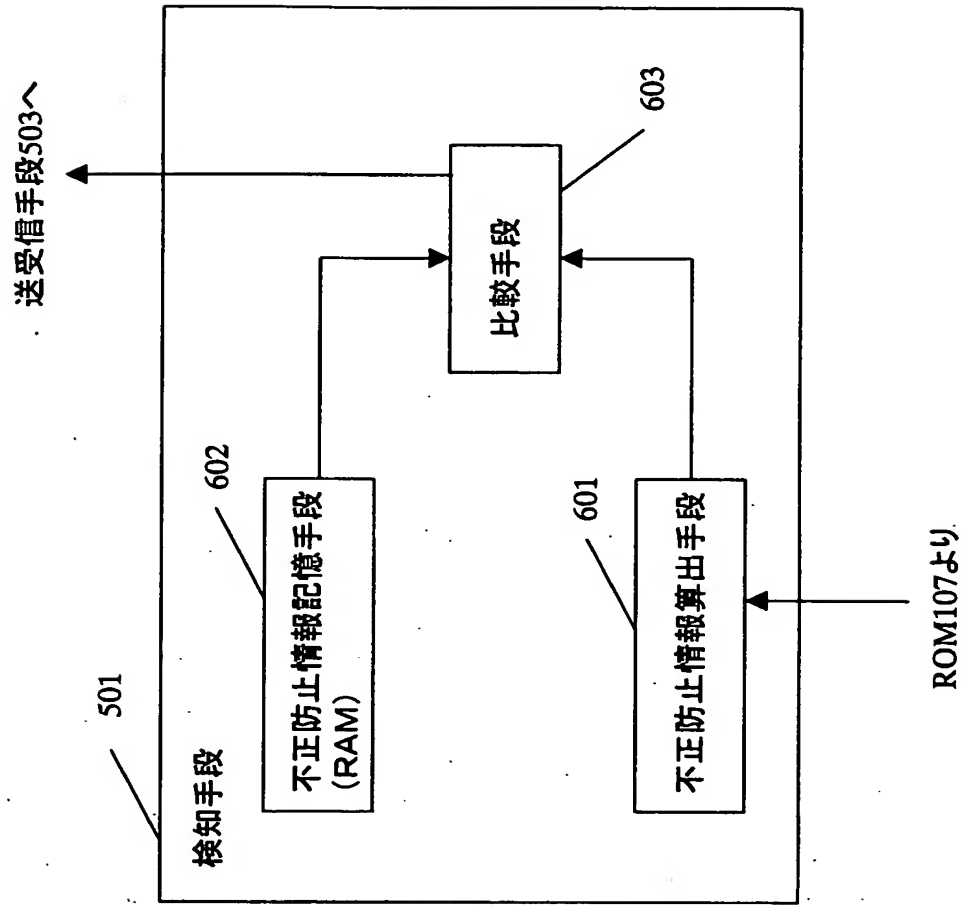
【図 4】



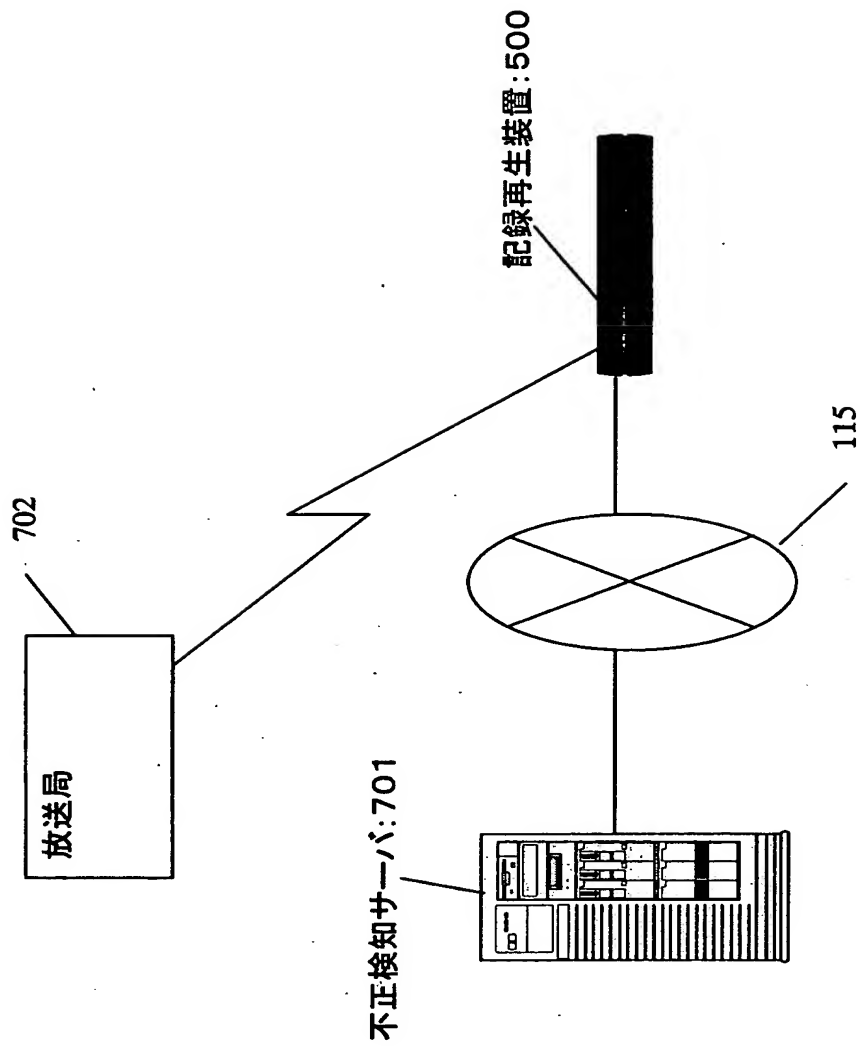
【図 5】



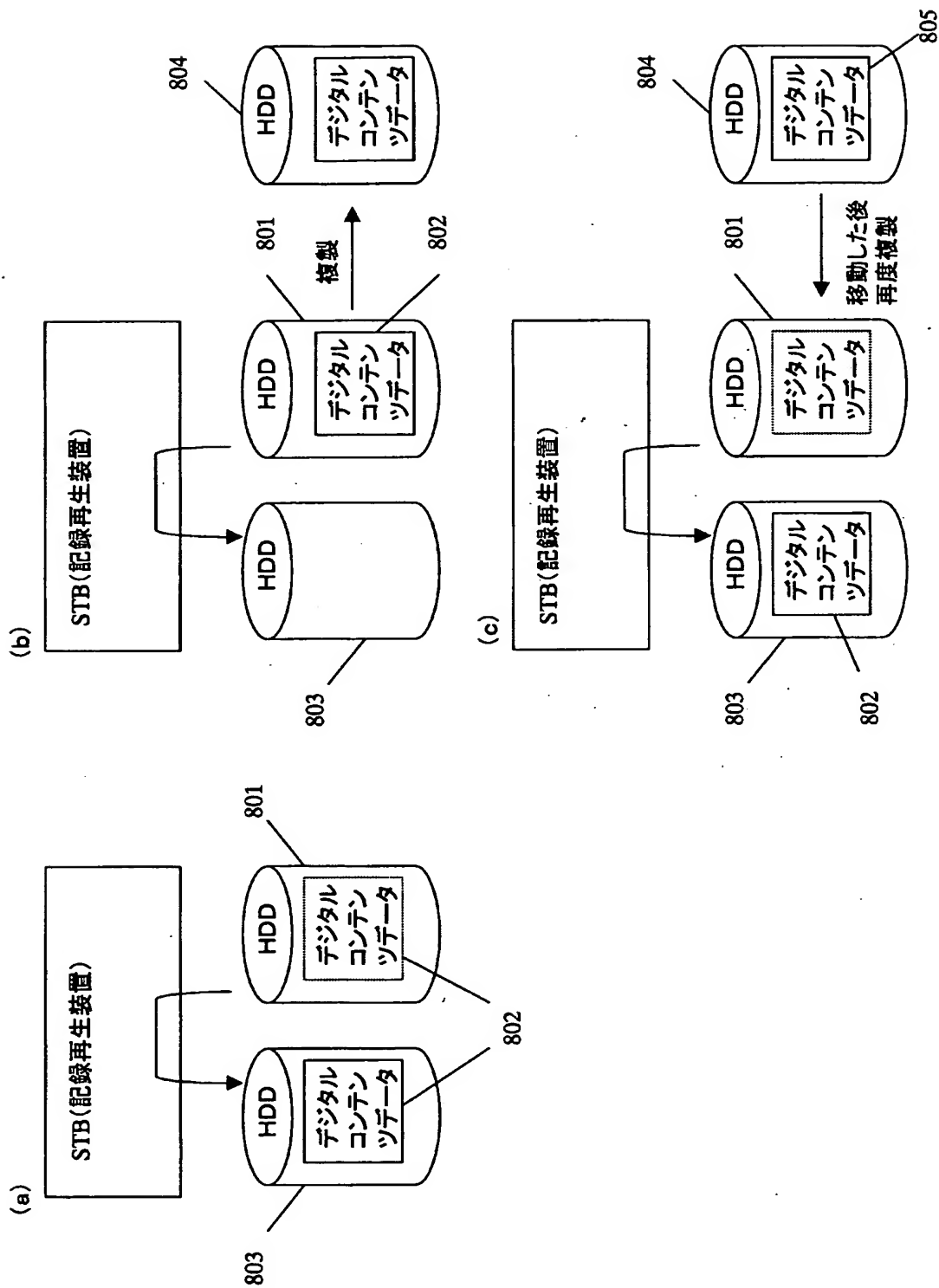
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 著作権を有する情報が不正に利用された際に当該不正を検出し、必要に応じて不正が行われた機器を無効化することにより、一層強固に著作権を保護する記録再生装置を提供する。

【解決手段】 検知手段は、デジタルコンテンツデータ又は記録再生装置を制御する制御プログラムの不正利用を検知し、無効化手段は検知手段による不正利用の検知に基づいて当該記録再生装置の利用を停止する記録再生装置を提供する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社